Release Notes for Cisco 2500 Series for Cisco IOS Release 12.0 T

December 13, 1999

These release notes for Cisco 2500 series support Cisco IOS Release 12.0 T, up to and including Release 12.0(7)T. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode or modem code and related documents.

For a list of the software caveats that apply to Release 12.0(7)T, see the *Caveats for Cisco IOS Release 12.0 T* document that accompanies these release notes. The caveats document is updated for every maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.0* on CCO and the Documentation CD-ROM.

Contents

These release notes describe the following topics:

- System Requirements, page 2
- New and Changed Information, page 18
- Important Notes, page 36
- Caveats, page 42
- Related Documentation, page 43
- Obtaining Documentation, page 48
- Obtaining Technical Assistance, page 48

CISCO SYSTEMS

Corporate Headquarters: Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 1999–2000. Cisco Systems, Inc. All rights reserved.

System Requirements

This section describes the system requirements for Release 12.0 T:

- Memory Requirements, page 2
- Hardware Supported, page 3
- Determining the Software Version, page 4
- Upgrading to a New Software Release, page 4
- Feature Set Tables, page 4

Memory Requirements

Table 1 Memory Requirements for Cisco 2500 Series Routers

Feature Sets[1]	Image Name	Software Image	Required Flash Memory	Required DRAM Memory	Runs from	In[2]
IP Feature Sets	IP	c2500-i-l	8 MB	6[6] MB	Flash	
	IP/FW	c2500-io-l	8 MB	8[3] MB	Flash	
	IP/FW Plus IPSec 56	c2500-ios56i-l	16 MB	10[4] MB	Flash	
	IP Plus	c2500-is-l	16[5] MB	8[6] MB	Flash	
	IP Plus 40[7]	c2500-is40-l	16[5] MB	10[6] MB	Flash	
	IP Plus 56[7]	c2500-is56-l	16[5] MB	10[3] MB	Flash	
	IP Plus IPSec 56	c2500-is56i-l	16 MB	10[3] MB	Flash	
	IP/H323	c2500-ix-l	8 MB	16 MB	Flash	(4)
	IP/IBM/APPN[7]	c2500-ai3r4-l	16 MB	8 MB	Flash	
	IP/IPX/AT/DEC	c2500-d-l	16 MB	6[6] MB	Flash	
	IP/IPX/AT/DEC/FW Plus	c2500-dos-l	16 MB	10[8] MB	Flash	
	IP/IPX/AT/DEC Plus	c2500-ds-l	16 MB	8[9] MB	Flash	
Enterprise Feature Sets	Enterprise/APPN Plus IPSec 56[7]	c2500-ajs56i-l	16 MB	16[4] MB	Flash	
	Enterprise/FW Plus IPSec 56	c2500-jos56i-l	16 MB	16[4] MB	Flash	
	Enterprise Plus	c2500-js-l	16 MB	10[3] MB	Flash	
	Enterprise Plus IPSec 56	c2500-js56i-l	16 MB	16[4] MB	Flash	
FRAD Feature Sets	FRAD	c2500-f-l	8 MB	8[3] MB	Flash	
	LAN FRAD/OSPF	c2500-f2in-l	8 MB	8[3] MB	Flash	
	LAN FRAD	c2500-fin-l	8 MB	8[3] MB	Flash	
	Remote Access Server (RAS)	c2500-c-l	8 MB	8[3] MB	Flash	
	ISDN	c2500-g-l	8 MB	8[3] MB	Flash	
	Distributed Director	c2500-w3-l	8 MB	4 MB	Flash	

1. If you need to upgrade the main memory for your Cisco series router, be sure to order the upgrade specific to your router.

2. The number in the "In" column indicates the Cisco IOS release when the image was first introduced. For example, (4) means an image was introduced in Release 12.0(4)T. If a cell in this column is empty, the interface was included in the initial base release.
3. 6 MB in Release 12.0(4)T. 4 MB in Release 12.0(3)T and earlier releases.
4. 8 MB in Release 12.0(4)T and earlier releases.
5. 8 MB in Releases 12.0(3)T and earlier releases.
6. 4 MB in Release 12.0(4)T and earlier releases.
7. This image is only available in Release 12.0(5)T and earlier releases.
8. 6 MB in Release 12.0(4)T and earlier releases.
9. 6 MB in Release 12.0(3)T and earlier releases.

Hardware Supported

Cisco IOS Release 12.0 T supports the Cisco 2500 series:

- Single LAN routers—Models 2502, 2503, 2504, 2520, 2521, 2522 and 2523
- Mission-specific, entry-level routers—Models 2501CF, 2502CF, 2503I, 2504I, 2520CF, 2520LF, 2521CF, 2521LF, 2522CF, 2522LF, 2523CF and 2523LF
- Router/hub combinations—Models 2505, 2507 and 2516
- Access servers—Models 2509 to 2512
- Dual LAN routers—Models 2513, 2514 and 2515
- Modular routers—Models 2524 and 2525 (optional integrated DSU/CSU or NT-1)

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 18.

Table 2 Supported Interfaces for the Cisco 2500 Series

Interface, Network Module, or Data Rate	Product Description	Platforms Supported
LAN Interfaces	Ethernet (AUI)	Cisco 2501, 2503, 2509, 2511, 2513, 2514, 2520, 2522, and 2524 only
	Ethernet (10BaseT)	Cisco 2505, 2507, 2516, and 2524 only
	4-Mbps Token Ring	Cisco 2502, 2504, 2513, 2515, 2521, 2523, and 2525 only
	16-Mbps Token Ring	Cisco 2502, 2504, 2513, 2515, 2521, 2523, and 2525 only)
WAN Data Rates	48/56/64 kbps	Cisco 2500 series
	128 kbps	Cisco 2500 series
	1.544/2.048 Mbps	Cisco 2500 series

Table 2 Supported Interfaces for the Cisco 2500 Series (continued)

Interface, Network Module, or Data Rate	Product Description	Platforms Supported
WAN Interfaces	EIA/TIA-232	Cisco 2500 series
	EIA/TIA-449	Cisco 2500 series
	EIA-530	Cisco 2500 series
	X.21	Cisco 2500 series
	V.35	Cisco 2500 series
	Serial, synchronous	Cisco 2500 series
	Serial, synchronous, and asynchronous	Cisco 2520, 2521, 2522, and 2523 only
	ISDN BRI S/T	Cisco 2503, 2504, 2516, 2520, 2521, 2522, 2523, 2524, and 2525 only
	ISDN BRI U	Cisco 2524 and 2525 only

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco 2500 series, log in to the router and enter the **show version** EXEC command:

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-DOS-L), Version 12.0(7)T, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For information on upgrading to a new software release, see the product bulletin *Cisco IOS Software Release 12.0 T Upgrade Paths and Packaging Simplification (#819: 1/99)* on CCO at:

Technical Documents: **Product Bulletins**: **Software**

Under **Cisco IOS 12.0**, click **Cisco IOS Software Release 12.0 T Upgrade (#819: 1/99)**.

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features.

Release 12.0 T supports the same feature sets as Release 12.0, but Release 12.0 T can include new features supported by the Cisco 2500 series.

Table 3 Feature Sets Supported by the Cisco 2500 Series

Feature Set Image Names	Feature Set Matrix Term	Software Image	Platforms	In[1]
IP	Basic[2]	c2500-i-l	Cisco 2500 series	
IP/FW	Basic	c2500-io-l	Cisco 2500 series	

Table 3 Feature Sets Supported by the Cisco 2500 Series (continued)

Feature Set Image Names	Feature Set Matrix Term	Software Image	Platforms	In[1]
IP/FW Plus IPSec 56	Plus[3], IPSec 56[4]	c2500-ios56i-l	Cisco 2500 series	
IP Plus	Plus	c2500-is-l	Cisco 2500 series	
IP Plus 40[5]	Plus 40[6]	c2500-is40-l	Cisco 2500 series	
IP Plus 56[5]	Plus 56[7]	c2500-is56-l	Cisco 2500 series	
IP Plus IPSec 56	Plus, IPSec 56	c2500-is56i-l	Cisco 2500 series	
IP/H323	Basic	c2500-ix-l	Cisco 2500 series	(4)
IP/IBM/APPN[5]	Basic	c2500-ai3r4-l	Cisco 2500 series	
IP/IPX/AT/DEC	Basic	c2500-d-l	Cisco 2500 series	
IP/IPX/AT/DEC/FW Plus	Plus	c2500-dos-l	Cisco 2500 series	
IP/IPX/AT/DEC Plus	Plus	c2500-ds-l	Cisco 2500 series	
Enterprise/APPN Plus IPSec 56[5]	Plus, IPSec 56	c2500-ajs56i-l	Cisco 2500 series	
Enterprise/FW Plus IPSec 56	Plus, IPSec 56	c2500-jos56i-l	Cisco 2500 series	
Enterprise Plus	Plus	c2500-js-l	Cisco 2500 series	
Enterprise Plus IPSec 56	Plus, IPSec 56	c2500-js56i-l	Cisco 2500 series	
FRAD	Basic	c2500-f-l	Cisco 2501, 2502, Cisco 2520–2523	
LAN FRAD/OSPF	Basic	c2500-f2in-l	Cisco 2501, 2502, Cisco 2520–2523	
LAN FRAD	Basic	c2500-fin-l	Cisco 2501, 2502, Cisco 2520–2523	
Remote Access Server (RAS)	Basic	c2500-c-l	Cisco 2500 series	
ISDN	Basic	c2500-g-l	Cisco 2500 series	
Distributed Director	Basic	c2500-w3-l	Cisco 2501–2502	

1. The number in the “In” column indicates the Cisco IOS release when the image was first introduced. For example, (4) means an image was introduced in Release 12.0(4)T. If a cell in this column is empty, the interface was included in the initial base release.
2. This feature set is offered in the basic feature set.
3. This feature set is offered in the Plus feature set.
4. This feature set is offered in the encryption feature sets, which consist of IPSec 56-bit (Plus IPSec 56) data encryption feature sets.
5. This image is only available in Release 12.0(5)T and earlier releases.
6. This feature set is offered in the encryption feature sets, which consist of 40-bit (Plus 40) data encryption feature sets.
7. This feature set is offered in the encryption feature sets, which consist of 56-bit (Plus 56) data encryption feature sets.

Caution Cisco IOS images with strong encryption (including, but not limited to 168-bit (3DES) data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United

States may require an export license. Customer orders may be denied or subject to delay due to United States government regulations. When applicable, the purchaser or the user must obtain local import and use authorizations for all encryption strengths. Contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Table 4, Table 5, and Table 6 list the features and feature sets supported by the Cisco 2500 series in Cisco IOS Release 12.0 T and use the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.
- In—The number in the "In" column indicates the Cisco IOS release in which the feature was introduced. For example, (7) means a feature was introduced in Release 12.0(7)T. If a cell in this column is empty, the feature was included in the initial base release.

Note These feature set tables only contain a selected list of features. These tables are not cumulative— nor do they list all the features in each image.

Table 4 Feature List by Feature Set for the Cisco 2500 Series, Part 1

		Feature Sets						
Features	**In**	**IP**	**IP/FW**	**IP/FW Plus IPSec 56**	**IP Plus**	**IP Plus 40[1]**	**IP Plus 56[1]**	**IP Plus IPSec 56**
Connectivity								
Airline Product Set Enhancements	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DNS-Based X.25 Routing	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dynamic Multiple Encapsulations Protocol	(7)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
L2TP Dial-Out	(5)	No	No	Yes	Yes	Yes	Yes	Yes
RIP Enhancements	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IBM Support								
Bridging Code Rework		Yes	Yes	Yes	Yes	Yes	Yes	Yes
DLSw+ Enhancements	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DLSw+ Ethernet Redundancy	(5)	No	No	Yes	Yes	Yes	Yes	Yes
RIF Passthru in DLSw+		No	No	No	Yes	Yes	Yes	Yes
IP Routing								
Easy IP Phase 2-DHCP Server	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Flow WRED	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Type of Service and Precedence for GRE Tunnels		Yes	Yes	No	Yes	Yes	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco 2500 Series, Part 1 (continued)

Features	In	Feature Sets						
		IP	IP/FW	IP/FW Plus IPSec 56	IP Plus	IP Plus 40[1]	IP Plus 56[1]	IP Plus IPSec 56
IS-to-IS Multiarea Support	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF Point to Multipoint		Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF Packet Pacing	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Protocol-Independent Multicasts (PIM) Version 2		Yes	Yes	Yes	Yes	Yes	Yes	Yes
WCCP v2 Support	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Load Balancing	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Management								
Cisco IOS File System		Yes	Yes	Yes	Yes	Yes	Yes	Yes
CNS Client for IOS	(5)	No	No	No	No	No	No	No
Conditionally Triggered Debugging		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Entity MIB		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Expression MIB		Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN MIB RFC 2127	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Migration of Distributed Director	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multicast Routing Manager	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Process MIB	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Response Time Reporter Enhancements	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Service Assurance Agent	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP Manager		Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP v3	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Miscellaneous								
Low Latency Queuing	(7)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multicast Source Discovery Protocol	(7)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NetFlow Policy Routing	(7)	No	No	Yes	Yes	Yes	Yes	Yes
SNA Switching Service	(7)	No	No	Yes	Yes	Yes	Yes	Yes
X.25 Closed User Groups	(7)	No	No	Yes	Yes	No	No	Yes

Table 4 Feature List by Feature Set for the Cisco 2500 Series, Part 1 (continued)

Features	In	Feature Sets						
		IP	IP/FW	IP/FW Plus IPSec 56	IP Plus	IP Plus 40[1]	IP Plus 56[1]	IP Plus IPSec 56
X.25 Switch Local Acknowledgment	(7)	No	No	Yes	Yes	No	No	Yes
VPN Tunnel Management	(7)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Quality of Service								
CLI Search String	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Parse Bookmarks	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Subnetwork Bandwidth Manager	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Reliability								
Frame Relay End-to-End KeepAlive	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PGM Router Assist	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Remote Failure Detection	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Scalability								
Airline Product Set (ALPS)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
ALPS II - UTS Support	(1)	No	No	Yes	Yes	Yes	Yes	Yes
Security								
AAA Support for MS-CHAP		No	No	No	No	No	No	No
Additional Vendor-Proprietary RADIUS Attributes		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Authenticating ACL		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Automated Double Authentication		No	Yes	Yes	Yes	Yes	Yes	Yes
Context-Based Access Control (CBAC)		No	No	Yes	No	No	No	No
Certificate Authority Interoperability		No	No	No	No	No	No	Yes
Internet Key Exchange Security Protocol		No	No	No	No	No	No	Yes
IOS Firewall Feature Set	(5)	No	Yes	Yes	No	No	No	No
IPSec Network Security		No	No	No	No	No	No	Yes

Table 4 Feature List by Feature Set for the Cisco 2500 Series, Part 1 (continued)

Features	In	Feature Sets						
		IP	IP/FW	IP/FW Plus IPSec 56	IP Plus	IP Plus 40[1]	IP Plus 56[1]	IP Plus IPSec 56
Named Method Lists for AAA Authentication & Accounting		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Switching								
Cisco IOS STP Enhancements	(1)	No	No	Yes	Yes	Yes	Yes	Yes
WAN Optimization								
DRP Server Agent Enhancements		Yes	Yes	Yes	Yes	Yes	Yes	Yes
WAN Services								
Always On Dynamic ISDN		No	No	No	No	No	No	No
Annex G	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Async over UDP	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dialer Watch		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dynamic Multiple Encapsulations for Dial-in over ISDN	(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mobile IP	(1)	No	No	Yes	Yes	Yes	Yes	Yes
MPPC- MS PPP Compression		Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS Callback		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multiple ISDN Switch Types		Yes	Yes	Yes	Yes	Yes	Yes	Yes
National ISDN Switch Type		Yes	Yes	Yes	Yes	Yes	Yes	Yes
PPP Over Frame Relay	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Time-Based Access Lists	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VPDN MIB Feature		No	No	No	Yes	Yes	Yes	Yes

1. This feature set image is only available in Release 12.0(5)T and earlier releases.

Table 5 Feature List by Feature Set for the Cisco 2500 Series, Part 2

Features	In	Feature Sets IP/H.323	IP/IBM/ APPN[1]	IP/IPX/AT/ DEC	IP/IPX/AT/ DEC/ FW Plus	IP/IPX/AT/ DEC Plus	Enterprise/ APPN Plus IPSec 56[1]	Enterprise/ FW Plus IPSec 56
Connectivity								
Airline Product Set Enhancements	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DNS-Based X.25 Routing	(5)	Yes	No	Yes	Yes	Yes	Yes	Yes
Dynamic Multiple Encapsulations Protocol	(7)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
L2TP Dial-Out	(5)	No	No	No	Yes	Yes	Yes	Yes
RIP Enhancements	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IBM Support								
Bridging Code Rework		Yes	Yes	Yes	Yes	Yes	Yes	Yes
DLSw+ Enhancements	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DLSw+ Ethernet Redundancy	(5)	No	Yes	No	Yes	Yes	Yes	Yes
RIF Passthru in DLSw+		Yes	Yes	No	No	Yes	Yes	Yes
IP Routing								
Easy IP Phase 2-DHCP Server	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Flow WRED	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Type of Service and Precedence for GRE Tunnels		Yes	Yes	Yes	Yes	Yes	Yes	Yes
IS-to-IS Multiarea Support	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF Point to Multipoint		Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF Packet Pacing	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Protocol-Independent Multicasts (PIM) Version 2		Yes	Yes	Yes	Yes	Yes	Yes	Yes
WCCP v2 Support	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Load Balancing	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Management							Yes	
Cisco IOS File System		Yes	Yes	Yes	Yes	Yes		Yes
CNS Client for IOS	(5)	Yes	No	No	No	No	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 2500 Series, Part 2 (continued)

Features	In	Feature Sets						
		IP/H.323	IP/IBM/ APPN[1]	IP/IPX/AT/ DEC	IP/IPX/AT/ DEC/ FW Plus	IP/IPX/AT/ DEC Plus	Enterprise/ APPN Plus IPSec 56[1]	Enterprise/ FW Plus IPSec 56
Conditionally Triggered Debugging		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Entity MIB		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Expression MIB		Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN MIB RFC 2127	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Migration of Distributed Director	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multicast Routing Manager	(5)	No	No	Yes	Yes	Yes	Yes	Yes
Process MIB	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Response Time Reporter Enhancements	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Service Assurance Agent	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP Manager		Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP v3	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Miscellaneous								
Low Latency Queuing	(7)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multicast Source Discovery Protocol	(7)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NetFlow Policy Routing	(7)	No	No	No	Yes	Yes	Yes	Yes
SNA Switching Service	(7)	No	Yes	No	Yes	Yes	Yes	Yes
X.25 Closed User Groups	(7)	No	No	No	Yes	Yes	No	Yes
X.25 Switch Local Acknowledgment	(7)	No	No	No	Yes	Yes	No	Yes
VPN Tunnel Management	(7)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Reliability								
Frame Relay End-to-End KeepAlive	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PGM Router Assist	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Remote Failure Detection	(5)	Yes	No	Yes	Yes	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 2500 Series, Part 2 (continued)

Features	In	Feature Sets						
		IP/H.323	IP/IBM/ APPN[1]	IP/IPX/AT/ DEC	IP/IPX/AT/ DEC/ FW Plus	IP/IPX/AT/ DEC Plus	Enterprise/ APPN Plus IPSec 56[1]	Enterprise/ FW Plus IPSec 56
Quality of Service		Yes	Yes	Yes	Yes	Yes	Yes	Yes
CLI Search String	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Parse Bookmarks	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Subnetwork Bandwidth Manager	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Scalability							Yes	
Airline Product Set (ALPS)		Yes	No	Yes	Yes	Yes		Yes
ALPS II - UTS Support	(1)	Yes	No	No	Yes	Yes	Yes	Yes
Security							Yes	
AAA Support for MS-CHAP		Yes	No	No	No	No	Yes	Yes
Additional Vendor-Proprietary RADIUS Attributes		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Authenticating ACL		Yes	Yes	No	Yes	Yes	No	Yes
Automated Double Authentication		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Context-Based Access Control (CBAC)		Yes	No	No	No	Yes	Yes	No
Certificate Authority Interoperability		Yes	No	No	No	No	Yes	Yes
Internet Key Exchange Security Protocol		Yes	No	No	No	No	Yes	Yes
IOS Firewall Feature Set	(5)	No	No	No	Yes	No	No	Yes
IPSec Network Security		Yes	No	No	No	No	Yes	Yes
Named Method Lists for AAA Authentication & Accounting		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Switching								
Cisco IOS STP Enhancements	(1)	Yes	Yes	No	Yes	Yes	Yes	Yes
WAN Optimization								
DRP Server Agent Enhancements		Yes	No	No	Yes	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 2500 Series, Part 2 (continued)

Features	In	Feature Sets						
		IP/H.323	IP/IBM/ APPN[1]	IP/IPX/AT/ DEC	IP/IPX/AT/ DEC/ FW Plus	IP/IPX/AT/ DEC Plus	Enterprise/ APPN Plus IPSec 56[1]	Enterprise/ FW Plus IPSec 56
WAN Services								
Always On Dynamic ISDN		Yes	No	No	No	No	Yes	Yes
Annex G	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Async over UDP	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dialer Watch		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dynamic Multiple Encapsulations for Dial-in over ISDN	(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mobile IP	(1)	Yes	No	No	Yes	Yes	Yes	Yes
MPPC- MS PPP Compression		Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS Callback		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multiple ISDN Switch Types		Yes	Yes	No	Yes	Yes	Yes	Yes
National ISDN Switch Type		Yes	Yes	No	Yes	Yes	Yes	Yes
PPP Over Frame Relay	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Time-Based Access Lists	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VPDN MIB Feature		Yes	No	Yes	No	Yes	Yes	Yes

1. This feature set image is only available in Release 12.0(5)T and earlier releases.

Table 6 Feature List by Feature Set for the Cisco 2500 Series, Part 3

Features	In	Feature Set							
		Enter-prise Plus	Enter-prise Plus IPSec 56	FRAD	LAN/ FRAD/ OSPF	LAN/ FRAD	Remote Access Server	ISDN	Distri-buted Director
Connectivity									
Airline Product Set Enhancements	(5)	Yes	Yes	No	No	No	No	No	No
DNS-Based X.25 Routing	(5)	Yes	Yes	No	No	No	No	No	No

Table 6 Feature List by Feature Set for the Cisco 2500 Series, Part 3 (continued)

Features		Feature Set							
	In	Enter-prise Plus	Enter-prise Plus IPSec 56	FRAD	LAN/ FRAD/ OSPF	LAN/ FRAD	Remote Access Server	ISDN	Distri-buted Director
Dynamic Multiple Encapsulations Protocol	(7)	Yes	Yes	No	No	No	No	No	Yes
L2TP Dial-Out	(5)	Yes	Yes	No	No	No	Yes	No	No
RIP Enhancements	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
IBM Support									
Bridging Code Rework		Yes	Yes	Yes	Yes	Yes	No	Yes	No
DLSw+ Enhancements	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
DLSw+ Ethernet Redundancy	(5)	Yes	Yes	Yes	Yes	Yes	No	No	No
RIF Passthru in DLSw+		Yes	Yes	Yes	Yes	Yes	No	Yes	No
IP Routing									
Easy IP Phase 2-DHCP Server	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Flow WRED	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
IP Type of Service and Precedence for GRE Tunnels		Yes	Yes	No	No	No	Yes	Yes	No
IS-to-IS Multiarea Support	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
OSPF Point to Multipoint		Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
OSPF Packet Pacing	(1)	Yes	Yes	Yes	No	No	No	Yes	No
Protocol-Independent Multicasts (PIM) Version 2		Yes	Yes	Yes	No	No	No	No	No
WCCP v2 Support	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
X.25 Load Balancing	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Management									
Cisco IOS File System		Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
CNS Client for IOS	(5)	Yes	Yes	No	No	No	No	No	No
Conditionally Triggered Debugging		Yes	Yes	Yes	Yes	Yes	Yes	Yes	No

Table 6 Feature List by Feature Set for the Cisco 2500 Series, Part 3 (continued)

Features	In	Feature Set: Enterprise Plus	Enterprise Plus IPSec 56	FRAD	LAN/ FRAD/ OSPF	LAN/ FRAD	Remote Access Server	ISDN	Distributed Director
Entity MIB		Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Expression MIB		Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
ISDN MIB RFC 2127	(1)	Yes	Yes	No	No	No	No	Yes	No
Migration of Distributed Director	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Multicast Routing Manager	(5)	Yes	Yes	No	No	No	No	No	No
Process MIB	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Response Time Reporter Enhancements	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Service Assurance Agent	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
SNMP Manager		Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
SNMP v3	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Miscellaneous									
Low Latency Queuing	(7)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multicast Source Discovery Protocol	(7)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NetFlow Policy Routing	(7)	Yes	Yes	No	No	No	No	No	No
SNA Switching Service	(7)	Yes	Yes	Yes	No	Yes	No	No	No
X.25 Closed User Groups	(7)	Yes	Yes	No	No	No	No	No	No
X.25 Switch Local Acknowledgment	(7)	Yes	Yes	No	No	No	No	No	No
VPN Tunnel Management	(7)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Reliability									
Frame Relay End-to-End KeepAlive	(5)	Yes	Yes	Yes	Yes	Yes	Yes	No	No
PGM Router Assist	(5)	Yes	Yes	No	No	No	Yes	Yes	No
X.25 Remote Failure Detection	(5)	Yes	Yes	No	No	No	No	No	No

Table 6 Feature List by Feature Set for the Cisco 2500 Series, Part 3 (continued)

Features		Feature Set							
	In	Enter-prise Plus	Enter-prise Plus IPSec 56	FRAD	LAN/ FRAD/ OSPF	LAN/ FRAD	Remote Access Server	ISDN	Distri-buted Director
Quality of Service									
CLI Search String	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Parse Bookmarks	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Subnetwork Bandwidth Manager	(5)	Yes	Yes	No	No	No	No	Yes	No
Scalability									
Airline Product Set (ALPS)		Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
ALPS II - UTS Support	(1)	Yes	Yes	No	No	No	No	No	No
Security									
AAA Support for MS-CHAP		Yes	Yes	No	No	No	No	No	No
Additional Vendor-Proprietary RADIUS Attributes		Yes	Yes	Yes	Yes	Yes	No	Yes	No
Authenticating ACL		Yes	Yes	Yes	No	No	No	No	No
Automated Double Authentication		Yes	Yes	Yes	No	No	No	No	No
Context-Based Access Control (CBAC)		No	No	No	No	No	No	No	No
Certificate Authority Interoperability		No	Yes	No	No	No	No	No	No
Internet Key Exchange Security Protocol		No	Yes	No	No	No	No	No	No
IOS Firewall Feature Set	(5)	No	No	No	No	No	No	No	No
IPSec Network Security		No	Yes	No	No	No	No	No	No
Named Method Lists for AAA Authentication & Accounting		Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Switching									
Cisco IOS STP Enhancements	(1)	Yes	Yes	Yes	Yes	Yes	No	No	No

Table 6 Feature List by Feature Set for the Cisco 2500 Series, Part 3 (continued)

Features	In	Feature Set: Enterprise Plus	Enterprise Plus IPSec 56	FRAD	LAN/ FRAD/ OSPF	LAN/ FRAD	Remote Access Server	ISDN	Distributed Director
WAN Optimization									
DRP Server Agent Enhancements		Yes	Yes	Yes	No	No	No	No	No
WAN Services									
Always On Dynamic ISDN		Yes	Yes	No	No	No	No	No	No
Annex G	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Async over UDP	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Dialer Watch		Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Dynamic Multiple Encapsulations for Dial-in over ISDN	(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Mobile IP	(1)	Yes	Yes	No	No	No	No	No	No
MPPC- MS PPP Compression		Yes	Yes	Yes	Yes	Yes	No	Yes	No
MS Callback		Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Multiple ISDN Switch Types		Yes	Yes	Yes	No	No	Yes	No	No
National ISDN Switch Type		Yes	Yes	Yes	No	No	Yes	No	No
PPP Over Frame Relay	(1)	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Time-Based Access Lists	(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
VPDN MIB Feature		Yes	Yes	Yes	No	No	Yes	No	No

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 2500 series for Release 12.0 T:

New Software Features in Release 12.0(7)T

The following new software enhancements are supported by the Cisco 2500 series for Release 12.0(7)T and later releases:

One New Feature Set

One new feature set has been created for the Cisco 2500 series in Release 12.0(7)T:

- Distributed Director—c2500-w3-l

Dynamic Multiple Encapsulations for Dial-In over ISDN

The Dynamic Multiple Encapsulations feature allows incoming calls over ISDN to be assigned an encapsulation type such as Frame Relay, PPP, and X.25 based on calling line identification (CLID) or DNIS. It also allows various encapsulation types and per-user configurations on the same ISDN B channel at different times according to the type of incoming call.

The Dynamic Multiple Encapsulations feature allows per-user configuration for each dial-in caller on any ingress ISDN B channel on which encapsulation can be run independently from other B channels on the same ISDN link. The caller is identified by CLID (caller ID) or DNIS to ensure that only incoming calls with authorization and valid user profiles are accepted. When PPP is used, authentication and profile binding can also be done by PPP name.

In addition, a large set of user profiles can be stored in dialer profiles locally or on a remote AAA server. (For large scale dial-in, storing user-specific configurations on a remote server becomes necessary for enhancing expandability and local memory efficiency.) However, whether stored locally or on a remote AAA server, the user-specific encapsulation and configuration can be applied to individual B channels dynamically and independently.

Dynamic multiple encapsulation is especially important in Europe where ISDN is relatively inexpensive and maximum use of all 30 B channels on the same ISDN link is desirable. Further, the feature removes the need to statically dedicate channels to a particular encapsulation and configuration type, and improves channel usage.

Low Latency Queueing

The Low Latency Queueing feature brings strict priority queueing to Class-Based Weighted Fair Queueing (CBWFQ). Strict priority queueing allows delay-sensitive data, such as voice, to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic.

Without Low Latency Queueing, CBWFQ provides weighted fair queueing based on defined classes with no strict priority queue available for real-time traffic. CBWFQ allows you to define traffic classes and then assign characteristics to that class. For example, you can designate the minimum bandwidth delivered to the class during congestion.

For CBWFQ, the weight for a packet belonging to a specific class is derived from the bandwidth you assigned to the class when you configured it. Therefore, the bandwidth assigned to the packets of a class determines the order in which packets are sent. All packets are serviced fairly based on weight; no class of packets may be granted strict priority.This scheme poses problems for voice traffic that is largely intolerant of delay, especially variation in delay. For voice traffic, variations in delay introduce irregularities of transmission manifesting as jitter in the heard conversation.

The Low Latency Queueing feature provides strict priority queueing for CBWFQ, reducing jitter in voice conversations. Configured by the **priority** command, Low Latency Queueing enables use of a single, strict priority queue within CBWFQ at the class level, allowing you to direct traffic belonging to a class to the CBWFQ strict priority queue.

In the event of congestion, when the bandwidth is exceeded policing is used to drop packets. Voice traffic enqueued to the priority queue is UDP-based and therefore not adaptive to the early packet drop characteristic of Weighted Random Early Detection (WRED).

When congestion occurs, traffic destined for the priority queue is metered to ensure that the bandwidth allocation configured for the class to which the traffic belongs is not exceeded.

Multicast Source Discovery Protocol

Multicast Source Discovery Protocol (MSDP) connects multiple PIM sparse-mode (SM) domains. MSDP allows multicast sources for a group to be known to all rendezvous points (RPs) in different domains. Each PIM-SM domain uses its own RPs and need not depend on RPs in other domains. An RP runs MSDP over TCP to discover multicast sources in other domains.

An RP in a PIM-SM domain has an MSDP peering relationship with MSDP-enabled routers in another domain. The peering relationship occurs over a TCP connection, where primarily a list of sources sending to multicast groups is exchanged. The TCP connections between RPs are achieved by the underlying routing system. The receiving RP uses the source lists to establish a source path.

The purpose of this topology is to have domains discover multicast sources in other domains. If the multicast sources are of interest to a domain that has receivers, multicast data is delivered over the normal, source-tree building mechanism in PIM-SM.

MSDP is also used to announce sources sending to a group. These announcements must originate at the domain's RP.

MSDP depends heavily on (M)BGP for interdomain operation. You should run MSDP in your domain's RPs that act as sources, sending to global groups for announcement to the Internet.

NetFlow Policy Routing

IP policy routing now works with Cisco Express Forwarding (CEF), Distributed CEF (DCEF), NetFlow, and NetFlow with flow acceleration. IP policy routing was formerly supported only in fast-switching and process-switching. Now that policy routing is integrated into CEF, policy routing can be deployed on a wide scale and on high-speed interfaces.

SNA Switching Services

SNASw provides an easier way than earlier methods to design and implement networks with Systems Network Architecture (SNA) routing requirements. Previously, this network design was accomplished using Advanced Peer-to-Peer Networking (APPN) with full network node (NN) support in the Cisco router. This type of support provided the SNA routing functionality needed, but was inconsistent with the trends in Enterprise networks today. The corporate intranet is replacing the SNA WAN. Enterprises

are replacing their traditional SNA network with an IP infrastructure that supports traffic from a variety of clients, using a variety of protocols, requiring access to applications on a variety of platforms, including SNA applications on Enterprise servers.

While SNA routing is still required when multiple servers must be accessed, the number of nodes required to perform this function is decreasing as the IP infrastructure grows and as the amount of native SNA traffic in the network decreases.

SNASw enables an enterprise to develop their IP infrastructure, while meeting SNA routing requirements.

X.25 Closed User Groups

The X.25 specification for Closed User Groups (CUG):

- Provides an application access security service that restricts users who do not have subscribed access to the host location.
- Provides a privacy technique that you can use to create private subnets or virtual networks out of a public data network.

Note Previously, Cisco supported only the ability to specify the CUG value but did not enforce restriction. Cisco currently enforces this security restriction.

X.25 Switch Local Acknowledgment

Cisco offers an X.25 switch function that creates virtual connections (VC) by connecting channels between X.25 class services.

The following X.25 class services are supported:

- X.25, Connection-Mode Network Service (CMNS)
- X.25 over TCP (XOT)
- Switched Virtual Circuits (SVCs) and Permanent Virtual Circuits (PVCs) are both supported and can be switched to each other (converted).

The current Cisco implementation provides end-to-end acknowledgment, which means that flow control or window and packet size acknowledgment is between the originating and terminating data terminal equipment (DTE).

Acknowledgment is not local to the DTE and data communications equipment (DTE), and the overall effect is low throughput.

VPN Tunnel Management

The VPN Tunnel Management feature provides network administrators with two new functions for managing VPN tunnels:

- The ability to set a limit for the maximum number of allowed simultaneous VPN sessions
- The ability to prevent new sessions from being established on a VPN tunnel without disturbing the service of existing sessions (this function is called VPN tunnel soft shutdown)

These functions can be used on either end of a VPN tunnel—the Network Access Server (NAS) or on the home gateway.

When this feature is enabled, Multichassis Multilink PPP (MMP) Layer 2 Forwarding (L2F) tunnels can still be created and established.

New Software Features in Release 12.0(5)T

The following new software enhancements are supported by the Cisco 2500 series in Release 12.0(5)T and later releases.

Airline Product Set Enhancements

The Airline Product Set Enhancements feature, ALPS phase III, provides support for Mapping of Airline Traffic over Internet Protocol (MATIP). MATIP is an industry standard protocol for transporting airline protocol traffic across a TCP/IP network. This feature enables the end-to-end delivery of ALC and UTS data streams between a Cisco router and the mainframe using TCP/IP. This feature removes the X.25 (AX.25 or EMTOX) requirements for communication with the host reservation system by enabling TCP/IP communication between the router and the airline host reservation system.

CNS Client for Cisco IOS Software

Cisco Networking Services (CNS) Client feature for Cisco IOS software enables authenticated directory access. CNS Client for Cisco IOS software includes the following components:

- Lightweight Directing Access Protocol (LDAP) V.3 client
- Support to use Kerberos V.5 as security protocol for LDAP V.3 client
- CNS Event Services Client
- CNS Locator Services Client
- CNS IP Security (IPSec) virtual private network (VPN) Provisioning Agent
- CNS Configuration Change Notification Agent
- CNS Provisioning Agent

LDAP V.3 client functionality enables Cisco IOS software-based applications to securely authenticate to a CNS for Active Directory (CNS/AD) server using Kerberos V.5 as security protocol to retrieve or store information such as policy and configuration data. Cisco IOS software-based applications publish or subscribe to events using CNS event services client, enabling external applications using the application programming interface (API) features of CNS to receive events or publish events to the Cisco IOS device. This Cisco IOS software-based device will use CNS locator services client to locate the nearest directory server using Domain Name System. The administrator need not configure the device to locate the nearest directory server.

All the above-mentioned functionality is intended for use by internal Cisco IOS application developers. CNS IPSec VPN provisioning agent enables the router to retrieve IPSec policies stored in the CNS/AD server and configure itself, automating the provisioning of customer premises equipment devices for IPSec VPN. CNS provisioning agent enables Cisco IOS device to be provisioned using CNS event services.

DNS-Based X.25 Routing

Managing a large TCP/IP network requires accurate and up-to-date maintenance of IP addresses and X.121 address mapping information on each router database in the network. Currently, this data is managed manually. Because these addresses are constantly being added and removed in the network, the routing table of every router frequently needs to be updated, which is a time-consuming and error-prone task.

X.25 has long operated over an IP network, specifically using Transmission Control Protocol (TCP) as a reliable transport mechanism. This method is known as X.25 over TCP (XOT). However, large networks and financial legacy environments experienced problems with the amount of route configuration that needed to be performed manually because each router switching calls over TCP needed every destination configured. Every destination from the host router needed a static IP route statement, and for larger environments, these destinations could be as much as several thousand per router. Until now, the only way to map X.121 addresses and IP addresses was on a one-to-one basis using the **x25 route** *x121address* **xot** *ipaddress* command.

The solution to this problem was to centralize route configuration that routers could then access for their connectivity needs. This centralization is the function of the DNS-Based X.25 Routing feature, because the DNS server is a database of all domains and addresses on a network.

DSLw+ Ethernet Redundancy

The DLSw+ Ethernet Redundancy feature provides redundancy in an Ethernet environment. It enables DLSw+ to support parallel paths between two points in an Ethernet environment, ensuring resiliency in the case of a router failure and providing load balancing for traffic load.

DLSw+ could provide redundancy prior to this feature in a Token Ring environment or via backup peers. When an end station on an Ethernet LAN had multiple active paths into a DLSw+ network, problems occurred.

Redundancy is not possible in an Ethernet environment because, unlike Token Ring, it does not have a RIF field in its packet. The RIF notifies a router of the path a packet has traveled by tracking each ring number and bridge it travels along a path. If a bridge notices that the next ring matches a ring already in the RIF, then the frame is not copied on to that ring. The RIF prevents unreliable local reachability information, circuit contention, and undetected looping explorers.

Frame Relay End-to-End Keepalive

The Frame Relay End-to-End Keepalive feature enables the router to keep track of permanent virtual circuit (PVC) status, independent of the switches in the Frame Relay network. The routers at both ends of a PVC in a Frame Relay network engage in a keepalive session where one router issues keepalive messages and the router at the other end of the PVC connection responds. The time interval for the keepalive is configurable and is enabled on a per-PVC basis. As long as the keepalive-issuing router receives response messages, the PVC status is up. When response messages are not received (because of line failure, a faulty switch in the Frame Relay network, or a router failure), the PVC is down. This mechanism enables bidirectional communication of PVC status to both routers at the ends of a PVC connection.

Firewall Feature Set

The Cisco IOS Firewall feature set, available for a wide range of Cisco router platforms, adds greater depth and flexibility to existing Cisco IOS software security capabilities, enriching features such as authentication, encryption, and failover with robust firewall functionality and intrusion detection. A

Cisco IOS software-based, integrated firewall solution scales to meet the bandwidth and performance requirements of any network. It also maximizes a Cisco router investment by combining multiprotocol routing functionality with sophisticated security policy enforcement throughout the network.

The Cisco IOS Firewall feature set delivers cost-effective perimeter security packaged with advanced features like stateful, application-based filtering, dynamic per-user authentication and authorization, defense against network attacks, Java blocking, and real-time alerts. Because it is completely interoperable with Cisco IOS software features including NAT, VPN tunneling protocols, Cisco Express Forwarding (CEF), AAA extensions, Cisco encryption technology, and Cisco IOS IPSec, It is a complete, integrated VPN solution.

IS-to-IS Multiarea Support

As IS-to-IS networks grow, they are usually organized into a backbone area (Level 2) connected to local areas (Level 1). Routers establish Level 1 adjacencies to perform local area routing, and Level 2 adjacencies to perform routing between Level 1 areas. Previously, a Cisco router could route between the backbone (Level 2) area and at most a single Level 1 area.

The IS-IS Multiarea Support feature supports configuration of multiple Level 1 IS-to-IS areas on a single router. This configuration is especially useful in networks where devices support only Level 1 routing and are organized in a number of small Level 1 areas that cannot be aggregated for performance reasons.

Layer 2 Tunneling Protocol Dial-out

The Layer 2 Tunneling Protocol (L2TP) Dial-Out feature enables L2TP Network Servers (LNSs) to tunnel dial-out VPDN calls using L2TP as the tunneling protocol. This feature enables a centralized network to efficiently and inexpensively establish a virtual point-to-point connection with any number of remote offices.

Using the L2TP Dial-Out feature, Cisco routers can carry both dial-in and dial-out calls in the same L2TP tunnels.

Previously, only dial-in VPDN calls were supported.

L2TP dial-out involves two devices: an LNS and an L2TP Access Concentrator (LAC). When the LNS wants to perform L2TP dial-out, it negotiates an L2TP tunnel with the LAC. The LAC then places a PPP call to the client(s) the LNS wants to dial-out to.

Multicast Routing Monitor

The Multicast Routing Monitor (MRM) feature is a management diagnostic tool that provides network fault detection and isolation in a large multicast routing infrastructure. It is designed to notify a network administrator of multicast routing problems in near real time.

MRM has three components that play different roles: the Manager, the Test Sender, and the Test Receiver. The Manager can reside on the same device as the Test Sender or Test Receiver. You can test a multicast environment using test packets (perhaps before an upcoming multicast event), or you can monitor existing IP multicast traffic.

You create a test based on various test parameters, name the test, and start the test. The test runs in the background and the command prompt returns. If the Test Receiver detects an error (such as packet loss or duplicate packets), it sends an error report to the router configured as the Manager. The Manager immediately displays the error report. Also, by issuing a certain **show** command, you can see the error

reports, if any. You then troubleshoot your multicast environment as normal, perhaps using the **mtrace** command from the source to the Test Receiver. If the **show** command displays no error reports, the Test Receiver is receiving test packets without loss or duplicates from the Test Sender.

PGM Router Assist

The PGM Router Assist feature allows Cisco routers to support the optimal operation of Pragmatic General Multicast (PGM). The PGM Reliable Transport Protocol itself is implemented on the hosts of the customer.

PGM is a reliable multicast transport protocol for applications that require ordered, duplicate-free, multicast data delivery from multiple sources to multiple receivers. PGM guarantees that a receiver in a multicast group either receives all data packets from transmissions and retransmissions, or can detect unrecoverable data packet loss. PGM is intended as a solution for multicast applications with basic reliability requirements. It is network-layer independent; The Cisco implementation of the PGM Router Assist feature supports PGM over IP.

Service Assurance Agent

The Service Assurance (SA) Agent is both an enhancement to and a new name for the Response Time Reporter (RTR) feature that was introduced in Cisco IOS Release 11.2. The feature allows you to monitor network performance by measuring key Service Level Agreement metrics such as response time, network resources, availability, jitter, connect time, packet loss, and application performance.

With Cisco IOS Release 12.0(5)T, the SA Agent provides new capabilities that enable you to:

- Monitor the Domain Name Server, DHCP Server, and DLSw peer stack and tunnel performance. Thresholds can be used to trigger additional collection of time delay statistics.
- Monitor network one-way delay variance (jitter) and packet loss.
- Monitor web server response time.

Subnetwork Bandwidth Manager

Resource Reservation Protocol (RSVP) is a signalling mechanism that supports request of specific levels of service such as reserved bandwidth from the network. RSVP and its service class definitions are largely independent of the underlying network technologies. This independence requires that a user define the mapping of RSVP onto subnetwork technologies.

The Subnetwork Bandwidth Manager (SBM) feature answers this requirement for RSVP in relation to IEEE 802-based networks. SBM specifies a signalling method and protocol for LAN-based admission control for RSVP flows. SBM allows RSVP-enabled routers and Layer 2 and Layer 3 devices to support reservation of LAN resources for RSVP-enabled data flows. The SBM signalling method is similar to that of RSVP itself. SBM protocol entities have the following features:

- Reside in Layer 2 or Layer 3 devices.
- Can manage resources on a segment. A segment is a Layer 2 physical segment shared by one or more senders, such as a shared Ethernet or Token Ring wire.
- Can become candidates in a dynamic election process that designates one SBM as the segment manager. The elected candidate is called the Designated Subnetwork Bandwidth Manager (DSBM). The elected DSBM is responsible for exercising admission control over requests for resource reservations on a managed segment.

X.25 Remote Failure Detection

Static routes are used over a packet-switched data network in order to reduce volume-based costs of the network. Until now, if two routers were connected via multiple X.25 links (a primary and a secondary), a router could not detect failure of the primary link. If a failure occurred, the data was not transferred to the second link because X.25 was unable to determine whether remote links were up or down. Therefore X.25 could not use an alternate connection to a destination.

The X.25 Remote Failure Detection feature is important for X.25 users because now, after a primary link failure, the router can establish a secondary link and continue sending data. This feature is a way for the router to detect a call failure and to use a secondary route to send subsequent packets to the remote destination, at the same time as making periodic attempts to reconnect to its primary link.

New Software Features in Release 12.0(4)T

The following new software enhancements are supported by the Cisco 2500 series in Release 12.0(4)T and later releases.

One New Feature Set

One new feature set has been created for the Cisco 2500 series in Release 12.0(4)T:

- IP/H.323—c2500-ix-l

Dynamic Multiple Encapsulations for Dial-in over ISDN

The Dynamic Multiple Encapsulations feature allows incoming calls over Integrated Services Digital Network (ISDN) to be assigned an encapsulation type such as Point-to-Point Protocol (PPP), X.25, and ISDN Link Access Procedure, Balanced-Terminal Adapter (LAPB-TA) based on calling line identification (CLID) or Dialed Number Identification Service (DNIS). It also allows various encapsulation types as well as per-user configurations on the same ISDN B channel at different times according to the type of incoming call.

The Dynamic Multiple Encapsulations feature allows per-user configuration for each dial-in caller on any ingress ISDN B channel on which encapsulation can be run independently from other B channels on the same ISDN link. The caller is identified by CLID or DNIS to make sure that only incoming calls with authorization and valid user profiles are accepted. If the protocol is PPP, authentication and profile binding can also be done by PPP name.

Dynamic multiple encapsulations are especially important in Europe where ISDN is relatively inexpensive, and it is desirable to allow maximum use of all B channels on the same ISDN link, especially for large scale dial-in. Further, the feature removes the need to statically dedicate channels to a particular encapsulation and configuration type, and improves channel usage.

Although the Dynamic Multiple Encapsulations feature enhances large scale dial-in functionality, the feature also works well in smaller scale dial-in situations and for modem calls.

New Software Features in Release 12.0(3)T

The following new software enhancements are supported by the Cisco 2500 series in Release 12.0(3)T and later releases.

Annex-G (X.25 over Frame Relay)

Annex G (X.25 over Frame Relay) facilitates the migration from an X.25 backbone to a Frame Relay backbone by permitting encapsulation of CCITT X.25/X.75 traffic within a Frame Relay connection. Annex G has developed to accommodate the many Cisco customers in Europe, where X.25 still is a popular protocol. With Annex G, the process of transporting X.25 over Frame Relay has been simplified, by allowing direct X.25 encapsulation over a Frame Relay network.

This simple process is largely achieved using X.25 profiles (similar to dialer profiles), which were created to streamline the configuration of X.25 on a per DLCI basis. X.25 profiles can contain any existing X.25 command and, once created and named, can be simultaneously associated with more than one Annex G DLCI connection, just using the profile name.

CDP Additions for Cisco IOS

The Cisco Discovery Protocol (CDP) is a media-independent device discovery protocol that runs on all cisco manufactured equipment, including routers, bridges, access servers, and switches. Each device sends periodic messages to a multicast address. Each device listens to the periodic messages sent by others in order to learn about neighboring devices and determine when their interfaces to the media go up or down. With CDP, network management applications can learn the device type and the SNMP agent address of neighboring devices. This process enables applications to send SNMP queries to neighboring devices.

CDP runs on all media that support Subnetwork Access Protocol (SNAP), including local-area network (LAN), Frame Relay, and Asynchronous Transfer Mode (ATM) media. CDP runs over the data link layer only. Therefore, two systems that support different network-layer protocols can learn about each other.

Each device configured for CDP sends periodic messages to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime, information, which indicates the time a receiving device should hold CDP information before discarding it.

Additions for Cisco Discovery Protocol (CDP) include the following:

- new SYSLOG output for instances of mismatching native VLAN IDs (IEEE 802.1Q) on connecting ports and port duplex state values on connecting devices.
- **cdp advertise-v2** command and new output from **show cdp** commands

The benefits include, transparent support of X.25 encapsulation over the Frame Relay network; direct X.25 configurations on a per DLCI basis; multiple Annex G DLCIs can use the same X.25 profile; multiple logical X.25 SVCs per Annex G link, and the fact that Cisco routers already contain the functionality necessary to perform the framing and frame removal required by Annex G.

DistributedDirector

Cisco DistributedDirector provides dynamic, transparent, and scalable Internet traffic load distribution between multiple topologically dispersed servers. DistributedDirector is the only global Internet service scaling solution that utilizes Cisco Internetwork Operating System (Cisco IOS) software and leverages routing table information in the network infrastructure to make “network intelligent” load distribution decisions.

Using routing table intelligence in the network infrastructure, DistributedDirector transparently redirects end user service requests to the closest responsive server, as determined by client-to-server topological proximity and/or client-to-server response times, resulting in increased access performance seen by the end user and reduced transmission costs.

For Cisco IOS Release 12.0(3)T, the functionality of DistributedDirector from 11.1 IA is migrated to 12.0 T. Cisco DistributedDirector is only available as a special hardware/software bundle on the Cisco 2501, 2502, and the 4700-M platforms.

DLSw+ Enhanced Load Balancing

In a network with multiple capable paths, the DLSw+ Load Balancing Enhancements feature improves traffic load balancing between peers by distributing new circuits based on existing loads and the desired ratio.

For each capable peer (peers that have the lowest or equal cost specified), the DLSw+ Load Balancing feature calculates the difference between the desired and the actual ratio of circuits being used on a peer. It detects the path that is underloaded in comparison to the other capable peers and assigns new circuits to that path until the desired ratio is achieved.

DLSw+ Peer Clusters

The DLSw+ Peer Clusters feature reduces the explorer packet replication that typically occurs in a large DLSw+ Peer Group design, where there are multiple routers connected to the same LAN.

The DLSw+ Peer Clusters feature associates DLSw+ peers (that are connected to the same LAN) into logical groups. Once the multiple peers are defined in the same peer group cluster, the DLSw+ Border Peer recognizes that it does not have to forward explorers to more than one member within the same peer group cluster.

DLSw+ RSVP Bandwidth Reservation

The DLSw+ RSVP Bandwidth Reservation feature allows DLSw+ to reserve network bandwidth for the DLSw+ TCP connection between DLSw+ peers.

Although it has been possible in the past to reserve bandwidth for a particular existing DLSw+ peer connection through the RSVP CLI support in Cisco IOS software, the CLI required prior knowledge of the TCP ports for which the reservation was being made. Because DLSw+ uses one well-known port and one randomly assigned port, the reservation could not be made until after the peer connection was active.

The DLSw+ RSVP feature permits new DLSw+ peer connections to automatically request bandwidth reservations upon connection, thereby removing the need for user intervention after the peer is connected. This feature assures the reservation will survive a network or device failure and that the DLSw+ traffic carried over a TCP connection is not affected by congestion.

Fancy Queuing on Frame Relay for Cisco HDLC

In previous releases, when the **voice-encap** option was configured on Frame Relay or Cisco HDLC, all fancy queuing (such as weighted fair queuing, custom queuing, and priority queuing) on the interface was disabled, and queuing was handled on a first-come first-served (FCFS) basis. In this release, new enhancements have been made to support fancy queuing on Frame Relay and Cisco HDLC.

For Frame Relay, a new interface command, **frag-pre-queuing**, has been added that allows you to set the queuing to be performed after the data segmentation. The command is available for Frame Relay interfaces only. The syntax for this new command is the following:

frag-pre-queuing

no frag-pre-queuing

By default, this command is enabled, which allows only FCFS queuing at the interface level. If you enter **no frag-pre-queuing**, you can configure weighted fair queuing, custom queuing, or priority queuing at the interface level. Note that if you enter **no frag-pre-queuing**, you still must explicitly configure the fancy queuing type on the interface.

For HDLC encapsulation, the queuing now takes place after segmentation when the **voice-encap** option is entered. Weighted fair queuing, custom queuing, and priority queuing are now supported on an interface configured for Cisco HDLC.

Flow-based WRED

This feature provides a mechanism to penalize the flows that do not respond to Weighted Random Early Detection (WRED) drops. This feature is provided as an extension to the existing WRED functionality and can be turned on after WRED is turned on.

Flow-WRED ensures that no single flow can hog all the buffer resources at the output interface queue. With WRED alone, this can occur in the presence of traffic sources that do not back off during congestion. Flow-WRED maintains minimal information about the buffer occupancy per flow. Whenever a flow exceeds it's share of the output interface buffer resource the packets of the flow are penalized by increasing the probability of their drop (by WRED).

Large Scale Dialout

Large scale dialout eliminates the need to configure dialer maps on every network access server (NAS) for every destination. Instead, you create remote site profiles containing outgoing call attributes (telephone number, service type, maximum number of links, and so on) on an authentication, authorization, and accounting (AAA) server. The profile is downloaded by the NAS when packet traffic requires a call to be placed to a remote site. Large scale dialout also takes advantage of features previously only available for incoming calls, such as dialer and virtual profiles, Multichassis Multilink PPP (MMP) support, and the ability to use an AAA server to store dial out attributes. MMP allows NASes to be stacked together and appear as a single NAS chassis so that if one NAS fails, another NAS in the stack can accept calls. Additionally, large scale dialout addresses congestion management by seeking an uncongested, alternative NAS when the designated primary NAS experiences port congestion.

Multilink Inverse Multiplexer

The Multilink Point to Point Protocol (MLP) Inverse Multiplexer feature allows you to combine multiple T1/E1 lines in a Versatile Interface Processor (VIP) T1/E1 interface into a bundle that has the combined bandwidth of the multiple T1/E1 lines. This is done by using a VIP MLP link. You choose the number of bundles and the number of T1/E1 lines in each bundle. This allows you to increase the bandwidth of you network links beyond that of a single T1/E1 line without having to purchase a T3 line.

Multimedia Conference Manager

Use the Multimedia Conference Manager to enable your current internetwork to route bit-intensive data such as audio telephony, video and audio telephony, and data conferencing using existing telephone and ISDN links, without degrading the network's current level of service. The Multimedia Conference Manager feature provides H.323 application options previously unavailable. Using Multimedia Conference Manager, you can implement H.323-compliant applications on existing networks in an incremental fashion without upgrades. This feature also provides a rich list of networking capability, including:

- A means to implement Quality of Service (QoS), which is required for the successful deployment of H.323 applications.
- Inter-zone routing in the E.164 address space. When using H.323-ID format addresses, inter-zone routing is done through domain names.

The Multimedia Conference Manager feature provides network administration mechanisms to support H.323 applications without impacting the mission critical applications running on today's networks. Multimedia Conference Manager is implemented on Cisco IOS software. Multimedia Conference Manager provides the network administrator with these abilities:

- Identify H.323 traffic and apply appropriate policies
- Limit H.323 traffic on the local-area network (LAN) and wide-area network (WAN)
- Provide user accounting for records based on service utilization
- Insert QoS for the H.323 traffic generated by applications such as Voice over IP (VoIP), data conferencing, and video conferencing
- Implement security for H.323 communications

Multimedia Conference Manager has two principal functions: *gatekeeper* and *proxy.* This document describes the value of the Multimedia Conference Manager gatekeeper and proxy functions for end-to-end implementation of H.323-compliant multimedia applications. These functions are unique to Multimedia Conference Manager. Similar robust features are currently not available in other vendor solutions.

Gatekeeper subsystems provide:

- User authorization where authorization, authentication, and accounting (AAA) account holders are permitted to register and use the services of Multimedia Conference Manager
- Accounting using AAA call detail records
- Zone bandwidth management to limit the number of active sessions
- H.323 call routing
- Address resolution

Starting with Cisco IOS Releases 11.3(6)Q and 11.3(7)NA and later, you can configure Cisco gatekeepers to use the Cisco Hot Standby Routing Protocol (HSRP), so that when one gatekeeper fails, the standby gatekeeper assumes its role.

Proxy subsystems provide:

- H.323 traffic consolidation
- Tight bandwidth controls
- QoS mechanisms such as IP Precedence and RSVP
- Secure communication over extranets

Process MIB

The addition of the CISCO-PROCESS-MIB and changes to the CISCO-MEMORY-POOL-MIB allow the retrieval of additional CPU and memory statistics and their reporting by SNMP. The CISCO-PROCESS-MIB provides CPU 5-second, 1-minute, and 5-minute statistics. In addition, this MIB provides CPU utilization and memory allocation/deallocation statistics for each process on each CPU listed in the CISCO-PROCESS-MIB.

The CISCO-PROCESS-MIB is enabled when the first SNMP command is configured. The background statistics collection for VIP cards and the master CPU occurs even if the SNMP subsystem is not initialized.

Response Time Reporter Enhancements

The Response Time Reporter (RTR) feature allows you to monitor network performance, network resources, and applications by measuring response times and availability. RTR statistics can be used to perform troubleshooting, problem notifications and pre-problem analysis. The RTR enhancements extend IP support, such as Type of Service, and allow you to measure various types of IP traffic, such as UDP, TCP, and HTTP.

SLIP-PPP Banner and Banner Tokens

The SLIP-PPP Banner section of this feature enables you to configure the banner that is displayed when making a SLIP connection. This improves compatibility with non-Cisco SLIP dial-up software.

The Banner Tokens section of this feature introduces the use of tokens to all existing banner commands. Tokens allow you to display current information from the configuration, such as the router's hostname, IP address, encapsulation type, and MTU size.

SNMP v3

Simple Network Management Protocol version 3 (SNMPv3) addresses issues related to the large scale deployment of SNMP for configuration, accounting and fault management. Currently SNMP is predominantly used for monitoring and performance management. The primary goal of SNMPv3 is to define a secure version of the SNMP protocol. SNMPv3 also facilitates remote configuration of the SNMP entities which make remote administration of SNMP entities a much simpler task. SNMPv3 builds on top of SNMPv1 and SNMPv2 to provide a secure environment for the management of systems and networks.

SNMPv3 provides an identification strategy for SNMP devices to facilitate communication only between known SNMP strategy. Each SNMP device has an identifier called the SNMP EngineID which is a copy of SNMP. Each SNMP message contains an SNMP EngineID. SNMP communication is possible only if an SNMP entity knows the identity of its peer SNMP device.

SNMPv3 also contains a security model or security strategy that exists between an SNMP user and the SNMP group to which the user belongs. A security model may define the security policy within an administrative domain or a intranet. The SNMPv3 protocol consists of the specification for the User based Security Model (USM).

Definition of security goals where the goals of message authentication service includes the following protection strategies:

- **Modification of Information** or protection against some unauthorized SNMP entity altering in-transit SNMP messages generated on behalf of an authorized principal)

- **Masquerade** or protection against attempting management operations not authorized for some principal by assuming the identity of another principal that has the appropriate authorizations
- **Message Stream Modification** or protection against messages getting maliciously re-ordered, delayed or replayed in order to effect unauthorized management operations
- **Disclosure** or protection against eavesdropping on the exchanges between SNMP engines. Three different types of communication mechanisms are available for this protection strategy. They are:
  - communication without authentication and privacy (NoAuthNoPriv)
  - communication with authentication and without privacy (AuthNoPriv)
  - communication with authentication and privacy (AuthPriv)

Token Ring MPOA

Token Ring Multiprotocol over ATM (MPOA) allows Token Ring hosts in an ATM network to communicate over alternate paths (called shortcuts) through the ATM network, which bypasses intermediate router hops that would otherwise be encountered in the default path.

Token Ring MPOA is an extension to LAN Emulation (LANE). Using the Next Hop Resolution Protocol (NHRP), and MPOA server (MPS) on the router, and MPO clients (MPCs) on the ATM edge devices, a direct virtual channel connection (VCC) between the ingress and egress edge devices is established. Token Ring MPOA allows Token Ring LANE clients to forward unicast IP packets between subnets to other Token Ring LANE clients through this shortcut VCC path on the ATM network.

Web Cache Communications Protocol Version 2 (WCCPv2)

The Web Cache Communications Protocol enables Cisco IOS routing platforms to transparently redirect content requests (for example, web requests) from clients to a locally connected Cisco Cache Engine (or Cache Cluster) instead of the intended origin server. When a Cache Engine receives such a request, it attempts to service it from its own local cache if the requested information is present. If not, the Cache Engine issues its own request to the originally requested origin server to get the required information. When the Cache Engine retrieves the requested information, it forwards it to the requesting client and caches it to fulfill future requests, thus maximizing download performance and significantly reducing WAN transmission costs.

WCCPv2 provides enhancements to WCCPv1, including:

- Multihome router support enables multiple co-located, WCCP-enabled routers to share a cache cluster.
- Improved security enables MD5 digital signature authentication (RFC 1321) to be used in Cache Engine/WCCP router communications.
- Redirection of non-port 80 traffic enables WCCP-enabled routers to transparently redirect traffic based on any TCP port (for example, FTP and NNTP traffic), in addition to HTTP traffic. Cache Engine-side support for non-port 80 traffic will be provided in the future.
- Content bypass support—When a Cache Engine rejects a request and sends it back to the WCCP-enabled router, the router knows not to redirect the request to the Cache Engine again.
- Flexible content distribution within a cache cluster—Various hashing parameters can be used to determine content distribution within a cache cluster.

X.25 Load Balancing

As the number of users accessing the same host has grown, competition for these application resources has become a problem. Internet service providers (ISPs) have had to increase the number of users they could support by increasing the number of X.25 lines to the host.

In order to support a large number of virtual circuits (VCs) to a particular destination, configuration of more than one serial interface to that destination was needed. When a serial interface is configured to support X.25, there is a fixed number of VCs available for use.

Using a facility called “hunt-group” (the method for X.25 load balancing), a switch is able to view a pool of X.25 lines going to the same host as one address and assign VCs on an “idle logical channel” basis. With this feature, X.25 calls can be load-balanced among all configured outgoing interfaces to fully use and balance all managed lines. The benefits include, the choice of two load-balancing distribution methods (rotary or vc-count) and improved performance of serial lines.

New Software Features in Release 12.0(2)T

There are no new features supported by the Cisco 2500 series in Cisco IOS Release 12.0(2)T.

New Software Features in Release 12.0(1)T

The following new software enhancements are supported by the Cisco 2500 series in Release 12.0(1)T and later releases.

RSM/TR-VLAN

The Token Ring VLAN support on the Route Switch Module (RSM) enables a Catalyst 5000 switch to provide the functionality of bridging and multi-protocol routing for Token Ring VLANs. The installation of an RSM in a Catalyst 5000 supplements the existing switching capabilities with the functionality of a standalone router that performs inter-VLAN routing and bridging. If the Token Ring RSM is associated with a VIP2 board, it provides direct external network connections through a variety of media using the standard port adapters on the VIP2 and offers functionality similar to a Cisco 7500 series router.

The RSM module can either route or bridge Token Ring packets, thereby functioning as a router or as a bridge. In Cisco IOS Release 12.0(1)T, both APPN and DLSW+ are supported on the RSM's Token Ring VLANs. RSRB, however, is not supported on the RSM.

Mobile IP

Mobile IP provides users the freedom to roam beyond their home subnet while consistently maintaining their home IP address. This enables transparent routing of IP datagrams to mobile users during their movement, so that data sessions can be initiated to them while they roam; it also enables sessions to be maintained in spite of physical movement between points of attachment to the Internet or other networks. Cisco's implementation of Mobile IP is fully compliant with the Internet Engineering Task Force's (IETF's) proposed standard defined in Request for Comments (RFC) 2002.

Easy IP Phase 2-DHCP Server

With the introduction of Easy IP Phase 2, Cisco IOS software also supports Intelligent DHCP Relay functionality. A DHCP Relay Agent is any host that forwards DHCP packets between clients and servers. A DHCP Relay Agent enables the client and server to reside on separate subnets. If the Cisco IOS DHCP server cannot satisfy a DHCP request from its own database, it can forward the DHCP request to one or more secondary DHCP servers defined by the network administrator using standard Cisco IOS ip helper-address functionality.

Smart-init (Mars FE2P)

The smart-init feature is an extension to the existing memory split program of the Cisco IOS software running on Cisco 3600 series routers. It computes iomem size by looking at the network modules installed in the system and uses this iomem for carrying out the memory split. Also, compatibility with older IOS configurations is maintained by retaining support for the **memory-size** configuration command. The user can disable smart-init and set iomem percentage to the required value by issuing the **memory-size** configuration command.

OSPF Packet Pacing

The former OSPF implementation for sending update packets needed to be more efficient. Some update packets were getting lost in cases where the link was slow, a neighbor could not receive the updates fast enough, or the router was out of buffer space. For example, packets might be dropped if either of these topologies existed:

- A fast router was connected to a slower router over a point-to-point link.
- During flooding, several neighbors dumped updates to a single router at the same time.

OSPF update packets are now automatically paced by a delay of 33 milliseconds. Pacing is also added between retransmissions to increase efficiency and minimize lost retransmissions.

OSPF update and retransmission packets are sent more efficiently. Also, you can display the LSAs waiting to be sent out an interface.

Time-Based Access Lists

It is now possible to implement access lists based on the time of day. To do so, you create a time range that defines specific times of the day and week. The time range is identified by a name, and then referenced by a function, so that those time restrictions are imposed on the function itself.

Currently, IP and IPX extended access lists are the only functions that can use time ranges. The time range allows the network administrator to define when the permit or deny statements in the access list are in effect. Prior to this feature, access list statements were always in effect once they were applied. Both named or numbered access lists can reference a time range.

RIP Enhancements

Triggered extensions to IP RIP increase efficiency of RIP on point-to-point, serial interfaces.

Routers are used on connection-oriented networks to allow potential connectivity to many remote destinations. Circuits on the WAN are established on demand and are relinquished when the traffic subsides. Depending on the application, the connection between any two sites for user data could be short and relatively infrequent.

There were two problems using RIP to connect to a WAN:

- Periodic broadcasting by RIP generally prevented WAN circuits form being closed.
- Even on fixed, point-to-point links, the overhead of periodic RIP transmissions could seriously interrupt normal data transfer because of the quantity of information that hits the line every 30 seconds.

To overcome these limitations, triggered extensions to RIP cause RIP to send information on the WAN only when there has been an update to the routing database. Periodic update packets are suppressed over the interface on which this feature is enabled.

Cisco IOS Firewall Feature Set Platform Support

The Cisco IOS Firewall feature set is now available on 2600 and 3600 series products.

The Cisco IOS Firewall feature set extends the security technology currently available in Cisco IOS software to provide firewall specific capabilities:

- Context-based Access Control (CBAC)
- Java blocking
- Denial-of-service detection and prevention
- Real-time alerts and audit trails

The Cisco IOS Firewall feature set adds advanced filtering capabilities to existing security functionality in Cisco routers. Some existing Cisco IOS security features include packet filtering via access control lists (ACLs), Network Address Translation (NAT), network-layer encryption, and TACACS+ authentication.

ISDN MIB RFC2127

The new Integrated Services Digital Network (ISDN) Management Information Base (MIB) RFC2127 has been designed to provide useful information in accordance with the IETF's new standard for the management of ISDN interfaces. It controls all aspects of ISDN interfaces. RFC2127 provides information on the physical Basic Rate Interfaces (BRIs), control and statistical information for B (bearer) and D (signaling) channels, terminal endpoints, and directory numbers.

IOS STP Enhancements

IOS Spanning Tree Protocol enhancements broaden the original IOS STP implementation with increased port identification capability, improved path cost determination, and support for a new VLAN bridge spanning-tree protocol.

Layer Two Tunneling Protocol (L2TP)

Layer Two Tunneling Protocol (L2TP) is an emerging Internet Engineering Task Force (IETF) standard that combines the best features of two existing tunneling protocols: Cisco's Layer Two Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP is an extension to the Point-to-Point Protocol (PPP), which is an important component for Access Virtual Private Networks (VPNs). Access VPNs allow mobile users to connect to their corporate intranets or extranets, thus improving flexibility and reducing costs.

Traditional dial-up networking services only supported registered IP address, which limited the types of applications that could be implemented over Virtual Private Networks (VPNs). L2TP supports multiple protocols and unregistered and privately administered IP addresses over the Internet. This allows the existing access infrastructure, such as the Internet, modems, access servers, and ISDN terminal adaptors (TAs), to be used.

L2TP can be initiated wherever PPTP or L2F is currently deployed and can be operated as a client initiated tunnel, such as PPTP, or a network access server (NAS) initiated tunnel, such as L2F.

PPP Over Frame Relay

The PPP over Frame Relay feature allows a router to establish end-to-end Point-to-Point Protocol (PPP) sessions over Frame Relay. IP datagrams are transported over the PPP link using RFC 1973 compliant Frame Relay framing. This feature is useful for remote users running PPP to access their Frame Relay corporate networks.

PPP over Frame Relay provides the following benefits:

- Allows end-to-end PPP sessions over Frame Relay.
- Supports the 90i IDSL Channel Unit that supports both Frame Relay and Point-to-Point Protocol (PPP) on an ISDN DSL.

Data Compression Advanced Interface Module

This document describes how to configure, verify, and troubleshoot the Data Compression features of the Advanced Interface Module (AIM) on Cisco 2600 Series Routers. The Data Compression AIM provides hardware-based compression and decompression of packet data transmitted and received on the serial network interfaces of Cisco 2600 Series Routers without occupying the Port Module Slot, that might otherwise be used for additional customer network ports. Supported are the industry standard LZS and MPPC compression algorithms. The Data Compression AIM requires Cisco IOS Release 12.0(1)T, or later 12.0 T releases.

ATM PVC Trap Support

The ATM PVC Trap Support feature provides Simple Network Management Protocol (SNMP) notification for permanent virtual circuit (PVC) failures, and it provides SNMP access to PVC status tables.

Normally, a management station is not notified when an Asynchronous Transfer Mode (ATM) PVC goes down. The ATM PVC Trap Support feature enables an agent to send the required PVC traps for this notification. It also provides support for these PVC status tables: atmCurrentlyFailingPVclTable and atmInterfaceExtTable.

Important Notes

The following sections contain important notes about Cisco IOS Release 12.0 that can apply to the Cisco 2500 series.

Last Maintenance Release of Cisco IOS Release 12.0 T

Cisco IOS Release 12.0(6)T has been renamed 12.0(7)T to align this release with the 12.0(7) mainline release. The closed caveats for Release 12.0(7)T are identical to the caveats closed in the 12.0(7) mainline release. There was no change in the feature content of the renamed release—the features in 12.0(6)T are the same as 12.0(7)T. Release 12.0(7)T is the last maintenance release of the 12.0 T release train.

Customers needing closure of caveats for the 12.0 T features should migrate to the 12.1mainline release, which has the complete feature content of Release 12.0 T and will eventually reach General Deployment (GD). Release 12.0 T is a super set of the 12.0 mainline release, so all caveats closed in the 12.0 mainline are also closed in 12.0 T.

Caveat CSCdr91706 and IOS HTTP Vulnerability

A defect in multiple releases of Cisco IOS software will cause a Cisco router or switch to halt and reload if the IOS HTTP service is enabled, browsing to http://router-ip/anytext?/ is attempted, and the enable password is supplied when requested. This defect can be exploited to produce a denial of service (DoS) attack.

The vulnerability, identified as Cisco bug ID CSCdr91706, affects virtually all mainstream Cisco routers and switches running Cisco IOS software releases 12.0 through 12.1, inclusive. This is not the same defect as CSCdr36952.

The vulnerability has been corrected and Cisco is making fixed releases available for free to replace all affected IOS releases. Customers are urged to upgrade to releases that are not vulnerable to this defect as shown in detail below.

This vulnerability can only be exploited if the enable password is known or not set.

You are strongly encouraged to read the complete advisory, which is available at http://www.cisco.com/warp/public/707/ioshttpserverquery-pub.shtml .

Cisco IOS Syslog Failure

Certain versions of Cisco IOS software may fail or hang when they receive invalid User Datagram Protocol (UDP) packets sent to their syslog ports (port 514). At least one commonly used Internet scanning tool generates packets that cause such problems. This fact has been published on public Internet mailing lists, which are widely read both by security professionals and by security crackers. This information should be considered in the public domain.

Attackers can cause Cisco IOS devices to repeatedly fail and reload, resulting in a completely disabled Cisco IOS device that needs to be reconfigured by its administrator. Some Cisco IOS devices have been observed to hang instead of failing when attacked. These devices do not recover until they are manually restarted by reset or power cycling. An administrator must personally visit an attacked, hung device to restart it, even if the attacker is no longer actively sending any traffic. Some devices have failed without providing stack traces; some devices may indicate that they were "restarted by power-on," even when that is not the case.

Assume that any potential attacker is likely to know that existence of this problem and the ways to exploit it. An attacker can use tools available to the public on the Internet and does not need to write any software to exploit the vulnerability. Minimal skill is required and no special equipment is required.

Despite Cisco specifically inviting such reports, Cisco has received no actual reports of malicious exploitation of this problem.

This vulnerability notice was posted on Cisco's World Wide Web site:

http://www.cisco.com/warp/public/770/iossyslog-pub.shtml

This information was also sent to the following e-mail and USENET news recipients:

- cust-security-announce@cisco.com
- bugtraq@netspace.org
- first-teams@first.org (includes CERT/CC)
- first-info@first.org
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- nanog@merit.edu

Affected Devices and Software Versions

Vulnerable devices and software versions are specified in Table 7, *Affected and Repaired Software Versions.* Affected versions include Releases 11.3 AA, 11.3 DB, and all 12.0 versions (including 12.0 mainline, 12.0 S, 12.0 T, and any other regular released version whose number starts with 12.0), up to the repaired releases listed in Table 7. Cisco is correcting the problem in certain special releases and will correct it in future maintenance and interim releases. See Table 7, *Affected and Repaired Software Versions* for details. Cisco intends to provide fixes for all affected IOS variants.

No particular configuration is needed to make a Cisco IOS device vulnerable. It is possible to filter out attack traffic by using access lists. See the "Workarounds" section on page 39 for techniques. However, except at Internet firewalls, the appropriate filters are not common in customer configurations. Carefully evaluate your configuration before assuming that any filtering you have protects you against this attack.

The most commonly used or asked-about products are listed below. If you are unsure whether your device is running Cisco IOS software, log in to the device and issue the **show version** command. Cisco IOS software will identify itself simply as "IOS" or "Internetwork Operating System Software". Other Cisco devices will not have the **show version** command, or they will identify themselves differently in their output. The most common Cisco devices that run Cisco IOS software include the following:

- Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 800, uBR900, 1000, 2500, 2600, 3000, 3600, 3800, 4000, 4500, 4700, AS5200, AS5300, AS5800, 6400, 7000, 7200 (including the uBR7200), 7500, and 12000 series
- Most recent versions of the LS1010 ATM switch
- Some versions of the Catalyst 2900XL LAN switch

- Cisco DistributedDirector

Affected software versions, which are relatively new, are not necessarily available on every device listed above. If you are not running Cisco IOS software, you are not affected by this problem.

The following Cisco devices are *not* affected:

- 700 dialup routers (750, 760, and 770 series)
- Catalyst 1900, 2800, 2900, 3000, and 5000 LAN switches are not affected, except for some versions of the Catalyst 2900XL. However, optional router modules running Cisco IOS software in switch backplanes, such as the RSM module for the Catalyst 5000 and 5500, are affected.
- WAN switching products in the IGX and BPX lines
- MGX (formerly known as the AXIS shelf)
- Host-based software
- Cisco PIX Firewall
- Cisco LocalDirector
- Cisco Cache Engine

This vulnerability has been assigned Cisco bug ID CSCdk77426.

Solution

Cisco offers free software updates to correct this vulnerability for all affected customers—regardless of their contract status. However, because this vulnerability information has been disseminated by third parties, Cisco has released this notice before updates are available for all software versions. Table 7 gives Cisco's projected fix dates.

Make sure your hardware has adequate RAM to support the new software before installing it. The amount of RAM is seldom a problem when you upgrade within a major release (say, from 11.2[11]P to 11.2[17]P), but it is often a factor when you upgrade between major releases (say, from 11.2 P to 11.3 T).

Because fixes will be available for all affected releases, this vulnerability will rarely, if ever, require an upgrade to a new major release. Cisco recommends very careful planning for any upgrade between major releases. Make certain no known bugs will prevent the new software from working properly in your environment.

Further upgrade planning assistance is available on Cisco's World Wide Web site at:

http://www.cisco.com

If you have service contracts you can obtain new software through your regular update channels (generally through Cisco's World Wide Web site). You can upgrade to any software release, but you must remain within the boundaries of the feature sets you have purchased.

If you do not have service contracts, you can upgrade to obtain only the bug fixes; free upgrades are restricted to the minimum upgrade required to resolve the defects. In general, you will be restricted to upgrading within a single row of Table 7, except when no upgrade within the same row is available in a timely manner. Obtain updates by contacting one of the following Cisco Technical Assistance Centers (TACs):

- +1 800 553 2447 (toll-free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- tac@cisco.com

Give the URL of this notice (http://www.cisco.com/warp/public/770/iossyslog-pub.shtml) as evidence for a free update. Non-contract customers must request free updates through the TAC. Please do not contact either “psirt@cisco.com” or “security-alert@cisco.com” for software updates.

Workarounds

You can work around this vulnerability by preventing any affected Cisco IOS device from receiving or processing UDP datagrams addressed to its port 514. This can be done either by using packet filtering on surrounding devices, or by using input access list filtering on the affected IOS device itself.

If you use an input access list, apply that list to all interfaces to which attackers may be able to send datagrams. Interfaces include not only physical LAN and WAN interfaces but also virtual subinterfaces of those physical interfaces, as well as virtual interfaces and interface templates corresponding to GRE, L2TP, L2F, and other tunneling protocols.

The input access list must block traffic destined for UDP port 514 at any of the Cisco IOS device’s own IP addresses, as well as at any broadcast or multicast addresses on which the Cisco IOS device may be listening. Be sure to block both old-style “all-zeros” broadcasts and new-style “all-ones” broadcasts. It is not necessary to block traffic being forwarded to other hosts—only traffic actually addressed to the Cisco IOS device is of interest.

No single input access list works in all configurations. Know the effect of your access list in your specific configuration before activating it.

The following example shows a possible access list for a three-interface router, along with the configuration commands needed to apply the list. The example assumes input filtering is not needed, other than as a workaround for this problem:

```
! Deny all multicasts, and all unspecified-net broadcasts, to port 514
access-list 101 deny udp any 224.0.0.0 31.255.255.255 eq 514
! Deny old-style unspecified-net broadcasts
access-list 101 deny udp any host 0.0.0.0 eq 514
! Deny network-specific broadcasts. This example assumes that all of
! the local interfaces are on the class B network 172.16.0.0, subnetted
! everywhere with mask 255.255.255.0. This will differ from network
! to network. Note that we block both new-style and old-style broadcasts.
access-list 101 deny udp any 172.16.0.255 0.0.255.0 eq 514
access-list 101 deny udp any 172.16.0.0   0.0.255.0 eq 514
! Deny packets sent to the addresses of our own network interfaces.
access-list 101 deny udp any host 172.16.1.1 eq 514
access-list 101 deny udp any host 172.16.2.1 eq 514
access-list 101 deny udp any host 172.16.3.3 eq 514
! Permit all other traffic (default would be to deny)
access-list 101 permit ip any any

! Apply the access list to the input side of each interface
interface ethernet 0
ip address 172.16.1.1 255.255.255.0
ip access-group 101 in

interface ethernet 2
ip address 172.16.2.1 255.255.255.0
ip access-group 101 in

interface ethernet 3
ip address 172.16.3.3 255.255.255.0
ip access-group 101 in
```

Listing all possible addresses—especially all possible broadcast addresses—to which attack packets may be sent is complicated. If you do not need to forward any legitimate syslog traffic received on an interface, you can block all syslog traffic arriving on that interface. Remember that blocking will affect traffic routed through the Cisco IOS device as well as traffic destined to the device; if the IOS device is expected to forward syslog packets, you will have to do the detailed filtering. Because input access lists impact system performance, install them with caution—especially on systems running very near their capacity.

Software Versions and Fixes

Many Cisco software images have been or will be specially reissued to correct this vulnerability. For example, regular released Cisco IOS version 12.0(2) is vulnerable, as are interim versions 12.0(2.1) through 12.0(2.3). The first fixed interim version of Release12.0 mainline software is Release12.0(2.4). However, a special release, 12.0(2a), contains only the fix for this vulnerability and does not include any other bug fixes from later 12.0 interim releases.

If you are running Release 12.0(2) and want to fix this problem without risking possible instability presented by installing the 12.0(2.4) interim release, you can upgrade to Release 12.0(2a). Release 12.0(2a) is a "code branch" from the Release 12.0(2) base, which will merge back into the Release 12.0 mainline at Release 12.0(2.4).

Special releases, like 12.0(2a), are one-time, spot fixes, and they will not be maintained. Thus, the upgrade path from Release 12.0(2a) is to Release 12.0(3).

Table 7 specifies information about affected and repaired software versions.

Note All dates within this table are subject to change.

Table 7 Affected and Repaired Software Versions

Cisco IOS Major Release	Description	Special Fix[1]	First Fixed Interim Release[2]	Fixed Maintenance Release[3]
Unaffected Releases				
11.2 and earlier releases—all variants	Unaffected early releases (no syslog server)	Unaffected	Unaffected	Unaffected
11.3, 11.3 T, 11.3 DA, 11.3 MA, 11.3 NA, 11.3 WA, 11.3(2)XA	11.3 releases without syslog servers	Unaffected	Unaffected	Unaffected
Releases Based on 11.3				
11.3 AA	11.3 early deployment for AS58xx	11.3(7)AA2, 8-JAN-1999[4]	11.3(7.2)AA	11.3(8)AA, 15-FEB-1999
11.3 DB	11.3 for Cisco NRP routing blade in Cisco 6400 xDSL DSLAM			11.3(7)DB2, 18-JAN-1999
Releases Based on 12.0				
12.0	12.0 Mainline	12.0(2a), 8-JAN-1999	12.0(2.4)	12.0(3), 1-FEB-1999
12.0 T	12.0 new technology early deployment	12.0(2a)T1, 11-JAN-1999	12.0(2.4)T	12.0(3)T, 15-FEB-1999

Table 7 Affected and Repaired Software Versions (continued)

Cisco IOS Major Release	Description	Special Fix[1]	First Fixed Interim Release[2]	Fixed Maintenance Release[3]
12.0 S	ISP support; 7200, RSP, GSR		12.0(2.3)S, 27-DEC-1998	12.0(2)S[5], 18-JAN-1999
12.0 DB	12.0 for Cisco 6400 universal access concentrator node switch processor (lab use)			12.0(2)DB, 18-JAN-1999
12.0(1)W	12.0 for Catalyst 8500 and LS1010	12.0(1)W5(5a) and 12.0(1a)W5(5b) (LS1010 platform only)	12.0(1)W5(5.15)	12.0(1)W5(6) (platform support for Catalyst 8540M will be in 12.0(1)W5(7))
12.0(0.6)W5	One-time early deployment for CH-OC-12 module in Catalyst 8500 series switches	Unaffected; one-time release	Unaffected	Unaffected; To upgrade use 12.0(1)W5 releases.
12.0(1)XA3	Short-life release; merged to 12/0T at 12.0(2)T	Obsolete	Merged	Upgrade to 12.0(2a)T1 or to 12.0(3)T.
12.0(1)XB	Short-life release for Cisco 800 series; merged to 12.0 T and 12.0 (3)T	12.0(1)XB1	Merged	Upgrade to 12.0(3)T.
12.0(2)XC	Short-life release for new features in Cisco 2600, Cisco 3600, uBR7200, uBR900 series; merged to 12.0 T at 12.0(3)T	12.0(2)XC1, 7-JAN-1999	Merged	Upgrade to 12.0(3)T
12.0(2)XD	Short-life release for ISDN voice features; merged to 12.0 T at 12.0(3)T	12.0(2)XD1, 18-JAN-1999	Merged	Upgrade to 12.0(3)T
12.0(1)XE	Short-life release	12.0(2)XE, 18-JAN-1999	Merged	Upgrade to 12.0(3)T

1. A special fix is a one-time release that provides the most stable immediate upgrade path.
2. Interim releases are tested less rigorously than regular maintenance releases; interim releases can contain serious bugs.
3. Fixed maintenance releases are on a long-term upgrade path. Other long-term upgrade paths also exist.
4. All dates in this table are estimates and are subject to change.
5. This entry is not a misprint. The 12.0(2.3)S interim release is available before the 12.0(2)S regular release.

Deprecated MIBs

Old Cisco Management Information Bases (MIBs) will be replaced in a future release. OLD-CISCO-* MIBs are currently being migrated into more scalable MIBs—without affecting existing Cisco IOS products or NMS applications. You can update from deprecated MIBs to the replacement MIBs as shown inTable 8.

Table 8 Deprecated and Replacement MIBs

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	In development
OLD-CISCO-DECNET-MIB	
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

This section only contains open and resolved caveats for the current Cisco IOS maintenance release.

All caveats in Release 12.0 T are also in Release 12.0.

For information on caveats in Cisco IOS Release 12.0, see *Caveats for Cisco IOS Release 12.0*.

For information on caveats in Cisco IOS Release 12.0 T, see *Caveats for Cisco IOS Release 12.0 T*, which lists severity 1 and 2 caveats and is located on CCO and the Documentation CD-ROM.

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Software Center: Cisco IOS Software: Cisco IOS BugToolkit: Cisco Bug Navigator II**, or at http://www.cisco.com/support/bugtools

Related Documentation

The following sections describe the documentation available for the Cisco 2500 series. These documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on CCO and the Documentation CD-ROM.

Use these release notes with these documents:

- Release-Specific Documents, page 43
- Platform-Specific Documents, page 44
- Feature Modules, page 44
- Cisco IOS Software Documentation Set, page 44

Release-Specific Documents

The following documents are specific to Release 12.0 and are located on CCO and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.0*

  On CCO at:

  Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Release Notes: Cross-Platform Release Notes

  On the Documentation CD-ROM at:

  Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Release Notes: Cross-Platform Release Notes

- Product bulletins, field notices, and other release-specific documents on CCO at:

  Service & Support: Technical Documents

- *Caveats for Cisco IOS Release* 12.0 T

  This document contains caveats applicable to all platforms for all maintenance releases of Release 12.0 T.

  On CCO at:

  Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Caveats

  On the Documentation CD-ROM at:

  Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Caveats

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Software Center: Cisco IOS Software: Cisco IOS BugToolkit: Cisco Bug Navigator II**, or at http://www.cisco.com/support/bugtools

Platform-Specific Documents

These documents are available for the Cisco 2500 series on CCO and the Documentation CD-ROM:

- *Cisco 2524 and Cisco 2525 Public Network Certification*
- *Installing WAN Modules in the Cisco 2524 and Cisco 2525 Routers*
- *Cisco 2524 and Cisco 2525 Router User Guide*
- Release Notes for Cisco 2500 Series Routers
- *Redundant Power Systems*

On CCO at:

Technical Documents: Documentation Home Page: Access Servers and Access Routers: Modular Access Routers: Cisco 2500 Series Routers

On the Documentation CD-ROM at:

Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 2500 Series Routers

Feature Modules

Feature modules describe new features supported by Release 12.0 T and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: New Feature Documentation

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: New Feature Documentation

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents that are shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

Documentation Modules

Each module in the Cisco IOS documentation set consists of two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

On CCO and the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set.

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0:Configuration Guides and Command References

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References

Release 12.0 Documentation Set

Table 9 describes the contents of the Cisco IOS Release 12.0 software documentation set, which is available in electronic form and in printed form upon request.

Note You can find the most current Cisco IOS documentation on CCO and the Documentation CD-ROM. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0

Table 9 Cisco IOS Software Release 12.0 Documentation Set

Books	Chapter Topics
• *Configuration Fundamentals Configuration Guide* • *Configuration Fundamentals Command Reference*	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
• *Bridging and IBM Networking Configuration Guide* • *Bridging and IBM Networking Command Reference*	Transparent Bridging Source-Route Bridging Token Ring Inter-Switch Link Remote Source-Route Bridging DLSw+ STUN and BSTUN LLC2 and SDLC IBM Network Media Translation DSPU and SNA Service Point SNA Frame Relay Access Support APPN Cisco Database Connection NCIA Client/Server Topologies Cisco Mainframe Channel Connection Airline Product Set

Table 9 Cisco IOS Software Release 12.0 Documentation Set (continued)

Books	Chapter Topics
• *Dial Solutions Configuration Guide* • *Dial Solutions Command Reference*	X.25 over ISDN Appletalk Remote Access Asynchronous Callback, DDR, PPP, SLIP Bandwidth Allocation Control Protocol ISDN Basic Rate Service ISDN Caller ID Callback PPP Callback for DDR Channelized E1 & T1 Dial Backup for Dialer Profiles Dial Backup Using Dialer Watch Dial Backup for Serial Lines Peer-to-Peer DDR with Dialer Profiles DialOut Dial-In Terminal Services Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Dialup Networks Dial Business Solutions and Examples
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	Interface Configuration Overview LAN Interfaces Logical Interfaces Serial Interfaces
• *Network Protocols Configuration Guide, Part 1* • *Network Protocols Command Reference, Part 1*	IP Overview IP Addressing and Services IP Routing Protocols
• *Network Protocols Configuration Guide, Part 2* • *Network Protocols Command Reference, Part 2*	AppleTalk Novell IPX
• *Network Protocols Configuration Guide, Part 3* • *Network Protocols Command Reference, Part 3*	Network Protocols Overview Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• *Security Configuration Guide* • *Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Switching Services Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing

Table 9 Cisco IOS Software Release 12.0 Documentation Set (continued)

Books	Chapter Topics
• *Wide-Area Networking Configuration Guide* • *Wide-Area Networking Command Reference*	Wide-Area Network Overview ATM Frame Relay SMDS X.25 and LAPB
• *Voice, Video, and Home Applications Configuration Guide* • *Voice, Video, and Home Applications Command Reference*	Voice over IP Voice over Frame Relay Voice over ATM Voice over HDLC Frame Relay-ATM Internetworking Synchronized Clocks Video Support Universal Broadband Features
• *Quality of Service Solutions Configuration Guide* • *Quality of Service Solutions Command Reference*	Policy-Based Routing QoS Policy Propagation via BGP Committed Access Rate Weighted Fair Queueing Custom Queueing Priority Queueing Weighted Random Early Detection Scheduling Signaling RSVP Packet Drop Frame Relay Traffic Shaping Link Fragmentation RTP Header Compression
• *Cisco IOS Software Command Summary* • *Dial Solutions Quick Configuration Guide* • *System Error Messages* • *Debug Command Reference*	

Note *Cisco Management Information Base (MIB) User Quick Reference* is no longer published. For the latest list of MIBs supported by Cisco, see *Cisco Network Management Toolkit* on Cisco Connection Online. From CCO, click on the following path: **Service & Support: Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB**.

Obtaining Documentation

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly. Therefore, it is probably more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Registered Cisco.com users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at http://www.cisco.com/cgi-bin/subcat/kaojump.cgi.

Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the web, e-mail, a self-addressed stamped response card included in many printed documents, or by sending mail to Cisco.

Cisco.com

Cisco continues to revolutionize how business is done on the Internet. Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through Cisco.com, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access Cisco.com in the following ways:

- WWW: www.cisco.com
- Telnet: cco.cisco.com
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
  - From North America, call 408 526-8070
  - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using Cisco.com to cco-team@cisco.com.

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use www.cisco.com/techsupport.

To contact by e-mail, use one of the following:

Language	E-mail Address
English	tac@cisco.com
Hanzi (Chinese)	chinese-tac@cisco.com
Kanji (Japanese)	japan-tac@cisco.com
Hangul (Korean)	korea-tac@cisco.com
Spanish	tac@cisco.com
Thai	thai-tac@cisco.com

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml.

Software Configuration Tips on the Cisco Technical Assistance Center Home Page

If you have a Cisco.com log-in account, you can access the following URL, which contains links and tips on configuring your Cisco products:

http://www.cisco.com/public/technotes/tech_sw.html

This URL is subject to change without notice. If it changes, point your Web browser to Cisco.com, press **Login**, and click on this path: **Technical Assistance Center: Technical Tips.**

The following sections are provided from the Technical Tips page:

- Access Dial Cookbook—Contains common configurations or recipes for configuring various access routes and dial technologies.
- Field Notices—Notifies you of any critical issues regarding Cisco products and includes problem descriptions, safety or security issues, and hardware defects.
- Frequently Asked Questions—Describes the most frequently asked technical questions about Cisco hardware and software.
- Hardware—Provides technical tips related to specific hardware platforms.
- Hot Tips—Describes popular tips and hints gathered from the Cisco Technical Assistance Center (TAC). Most of these documents are available from the TAC Fax-on-demand service. To reach Fax-on-demand and receive documents at your fax machine from the United States, call 888-50-CISCO (888-502-4726). From other areas, call 650-596-4408.
- Internetworking Features—Lists tips on using Cisco IOS software features and services.
- Sample Configurations—Provides actual configuration examples that are complete with topology and annotations.

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate and value your comments.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 43.

AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco Net*Works* logo, the Cisco Powered Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare,FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, PIX, RateMUX, ScriptShare, SlideCast, SMARTnet, TransPath, Voice LAN, Wavelength Router, WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert Logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, IOS, IP/TV, LightStream, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0011R)

Copyright © 1999, Cisco Systems, Inc.
All rights reserved.